Nations Unies ECE/TRANS/WP.30/GE.1/2021/4

Conseil économique et social

Distr. générale
3 décembre 2020
Français
Original : anglais

Commission économique pour l'Europe

Comité des transports intérieurs

Groupe de travail des problèmes douaniers intéressant les transports

Groupe d'experts des aspects théoriques et techniques de l'informatisation du régime TIR

Première session
Genève, 27-29 janvier 2021
Point 6 a) de l'ordre du jour provisoire
Système international eTIR :
Rapport sur l'état d'avancement de l'élaboration du système international eTIR

Services Web eTIR − Aperçu général, sécurité et accès*

Note du secrétariat

I. Introduction − Mandat

1. À sa quatre-vingt-deuxième session (23-28 février 2020), le Comité des transports intérieurs a approuvé la création (ECE/TRANS/294, par. 84[1]) et le mandat (ECE/TRANS/WP.30/2019/9 et ECE/TRANS/WP.30/2019/9/Corr.1[2]) du Groupe d'experts des aspects théoriques et techniques de l'informatisation du régime TIR (WP.30/GE.1), décisions qui devaient être soumises à l'approbation du Comité exécutif de la CEE (EXCOM). À la réunion qu'il a tenue en ligne le 20 mai 2020, l'EXCOM a approuvé la mise en place du Groupe d'experts des aspects théoriques et techniques de l'informatisation du régime TIR (WP.30/GE.1), telle qu'approuvée dans le document ECE/TRANS/294, jusqu'en 2022, sur la base du mandat figurant dans le document ECE/TRANS/WP.30/2019/9 et son Corr.1 (ECE/EX/2020/L.2, al. b) du paragraphe 5[3]).

* Le présent document a été soumis tardivement aux services de traitement de la documentation en raison de contretemps liés à sa mise au point.

[1] Décision du Comité des transports intérieurs, par. 84 du document ECE/TRANS/294 (https://unece.org/fileadmin/DAM/trans/doc/2020/itc/ECE-TRANS-294f.pdf).

[2] Mandat du groupe nouvellement créé, approuvé par le Comité des transports intérieurs et le Comité exécutif (EXCOM) de la CEE (https://unece.org/fileadmin/DAM/trans/bcf/wp30/documents/2019/ECE-TRANS-WP30-2019-09f.pdf et rectificatif https://unece.org/DAM/trans/bcf/wp30/documents/2019/ECE-TRANS-WP30-2019-09c1f.pdf).

[3] Voir ECE/EX/2020/L.2, par. 5 b) (https://unece.org/DAM/commission/EXCOM/Agenda/2020/Remote_informal_mtg_20_05_2020/ Item_4_ECE_EX_2020_L.2_Mandates_fr.pdf).

2. Il est dit, dans le mandat du Groupe de travail, que celui-ci doit axer ses travaux sur l'élaboration d'une nouvelle version des spécifications eTIR, en attendant la mise en place de l'Organe de mise en œuvre technique (TIB). Le Groupe doit en particulier : a) établir une nouvelle version des spécifications techniques de la procédure eTIR, avec les modifications à y apporter, en veillant à assurer leur conformité avec les spécifications fonctionnelles de la procédure eTIR ; b) établir une nouvelle version des spécifications fonctionnelles de la procédure eTIR, avec les modifications à y apporter, en veillant à assurer leur conformité avec les spécifications conceptuelles de la procédure eTIR ; c) élaborer des amendements aux spécifications conceptuelles de la procédure eTIR, à la demande du WP.30.

3. Le présent document dresse un aperçu général des services Web eTIR, explique comment y accéder et fournit des détails sur la sécurité de la procédure eTIR, les aspects techniques de la mise en œuvre et l'essai des messages eTIR. Il est valable pour la version 1.0 du système international eTIR, fondée sur la version 4.3a des spécifications eTIR.

II. Objet

4. Le présent document décrit les services Web du système international eTIR, en particulier les destinataires visés, l'architecture du système, les différents messages et leurs séquences, les aspects relatifs à la sécurité, les accès ainsi que les interlocuteurs pour toute assistance. Il n'aborde pas en détail les exigences de mise en œuvre pour chaque message, que l'on peut consulter dans les documents consacrés à chacun des messages eTIR, mais décrit plutôt les éléments et processus à mettre en place dans les systèmes douaniers nationaux pour que ceux-ci puissent échanger efficacement avec le système international eTIR.

III. Destinataires

5. Ce guide est destiné aux équipes d'informaticiens des autorités douanières chargées d'interconnecter les systèmes douaniers nationaux au système international eTIR

IV. Conditions préalables

6. Avant de lire le présent document, il est nécessaire d'avoir au préalable assimilé les aspects théoriques du système eTIR[4] et lu et appliqué les Lignes directrices relatives au projet de connexion des services douaniers au système international eTIR[5]. Il est particulièrement important de bien comprendre les phases de mise en œuvre décrites dans les Lignes directrices et d'être conscient de la phase à laquelle on se trouve.

7. Pour que la mise en œuvre soit le plus efficace possible pour les autorités douanières, il est fortement recommandé que l'équipe informatique soit accompagnée d'un expert des questions liées au système TIR, comme indiqué dans les Lignes directrices relatives au projet de connexion des services douaniers au système international eTIR.

V. Présentation de la documentation sur le système eTIR

8. Étant donné que le système international eTIR se fonde sur la Convention TIR, la documentation relative au système eTIR s'appuie sur les articles et annexes de la Convention, mais aussi sur divers autres documents clefs accessibles en ligne qui sont présentés ci-dessous. Il est impératif de lire et de bien comprendre certains de ces documents, tandis que d'autres sont des documents de référence à consulter au besoin. Cette section permet de mieux comprendre ce que contiennent ces documents et dans quel ordre il est recommandé de les lire.

[4] www.unece.org/fileadmin/DAM/trans/bcf/adhoc/conc_tech/documents/id17-06e.pdf (en anglais seulement).

[5] wiki.unece.org/download/attachments/106299939/Project Guidelines for customs to connect to the eTIR international system.pdf (en anglais seulement).

a) Les Lignes directrices relatives au projet de connexion des services douaniers au système international eTIR : ce document, qui constitue le point de départ pour les autorités douanières de toute partie contractante, est à lire en premier.

Pour de plus amples informations sur les problématiques liées au transport et à la facilitation du passage des frontières, il est vivement conseillé de lire :

b) Le Manuel TIR[6], qui contient tous les éléments juridiques régissant la Convention TIR (y compris les commentaires et les notes explicatives) et présente le rôle des autorités douanières, des associations nationales et des titulaires de carnets TIR.

c) L'annexe 11 à la Convention TIR[7], qui décrit la procédure eTIR, explique comment les procédures seront adaptées pour être informatisées et définit le cadre juridique de la mise en place et de l'utilisation du système international eTIR.

9. Une fois que le cadre juridique et les principales procédures du régime TIR sont bien assimilées, il est fortement recommandé de lire :

d) L'introduction aux documents théoriques, fonctionnels et techniques relatifs au système eTIR[8], qui présente les documents théoriques, fonctionnels et techniques relatifs au projet d'informatisation du régime TIR conformément à la Méthode de modélisation du Centre des Nations Unies pour la facilitation du commerce et les transactions électroniques (CEFACT-ONU). Il s'agit du premier document à lire pour mieux percevoir comment le système eTIR a été imaginé comme un prolongement de la Convention TIR.

e) La présentation des aspects théoriques du système eTIR[9], dans laquelle sont décrits la logique et les concepts fondamentaux qui sous-tendent la mise en œuvre du système international eTIR. Il s'agit également d'un document de référence qui décrit tous les cas d'utilisation et toutes les règles suivies pour la mise en œuvre technique.

f) La présentation des spécifications fonctionnelles eTIR[10] est le document le plus important pour comprendre en profondeur les mécanismes employés pour mettre en œuvre le système international eTIR. La version actuelle (4.2) est développée dans un document de travail ({etir-spec-version}) et affinée au fur et à mesure des travaux et des enseignements tirés de la modélisation effectuée par le groupe spécial informel d'experts des aspects théoriques et techniques de l'informatisation du régime TIR (GE.1) et de tous les points de contact eTIR. Ces spécifications (auparavant intitulées Modèle de référence) renvoient également aux documents et listes supplémentaires suivants :

i) eTIR XML schemas (schémas XML eTIR)[11] ;

ii) eTIR code lists (listes de codes eTIR)[12] ;

iii) eTIR error code list (liste des codes d'erreur eTIR)[13].

g) Enfin, pour communiquer avec d'autres parties contractantes au cours de la mise en œuvre, on trouvera les coordonnées des points de contact eTIR[14] sur la page Web qui leur est consacrée.

[6] https://unece.org/DAM/tir/handbook/french/newtirhand/TIR-6Rev11f.pdf.

[7] https://unece.org/fileadmin/DAM/trans/bcf/ac2/documents/2020/ECE-TRANS-WP30-AC2-147f.pdf#page=22.

[8] www.unece.org/fileadmin/DAM/trans/bcf/adhoc/conc_tech/documents/id17-05e.pdf (en anglais seulement).

[9] www.unece.org/fileadmin/DAM/trans/bcf/adhoc/conc_tech/documents/id17-06e.pdf (en anglais seulement).

[10] www.unece.org/fileadmin/DAM/trans/bcf/adhoc/conc_tech/documents/id17-07e.pdf (en anglais seulement).

[11] wiki.unece.org/display/ED/Technical+artefacts (en anglais seulement).

[12] www.unece.org/fileadmin/DAM/trans/bcf/eTIR/documents/CodeLists0_4.pdf (en anglais seulement).

[13] wiki.unece.org/display/ED/Error+Management (en anglais seulement).

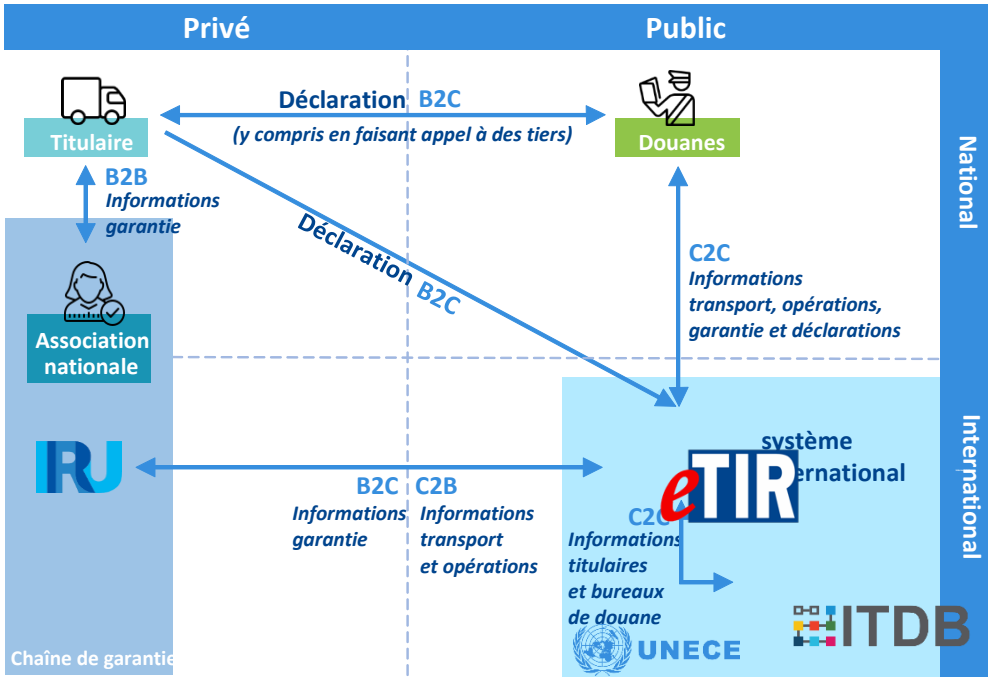
[14] https://unece.org/list-etir-focal-points (en anglais seulement).

VI. Aperçu général des services Web eTIR

A. Architecture de haut niveau

10. Le schéma ci-dessous représente le fonctionnement général du système international eTIR :

Figure I
Architecture de haut niveau du système eTIR



* Signification des sigles :
B2B : Relation d'entreprise à entreprise (le terme « entreprise » désignant une entité du secteur privé).
C2B : Relation de service douanier à entreprise (le terme « entreprise » désignant une entité du secteur privé).
B2C : Relation d'entreprise à service douanier (le terme « entreprise » désignant une entité du secteur privé).
C2C : Relation de service douanier à service douanier.

11. Outils techniques : le système international eTIR a été mis en œuvre en utilisant les éléments suivants :

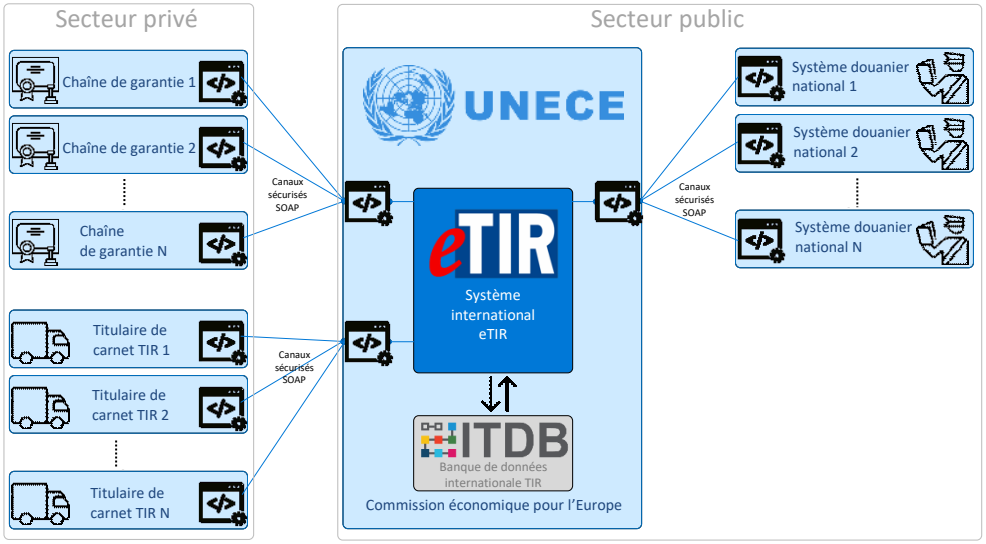
- Langage de programmation Java[15] ;
- Base de données PostgreSQL[16] ;
- Cadre Spring[17] ;
- ActiveMQ[18] ;
- Services Web SOAP-XML[19] ;
- Apache CXF[20] ;
- Apache Camel[21].

[15] docs.oracle.com/javase/7/docs/technotes/guides/language/.
[16] www.postgresql.org/.
[17] spring.io/.
[18] activemq.apache.org/.
[19] www.w3.org/TR/soap/.
[20] cxf.apache.org/.
[21] camel.apache.org/.

12. Ces outils ne sont mentionnés qu'à titre informatif. Pour toute question concernant les méthodes de mise en œuvre ou les outils techniques utilisés pour mettre en œuvre le système international eTIR, il convient de prendre contact avec les services d'assistance eTIR à l'adresse etir@un.org.

13. Le système international eTIR est accessible aux partenaires des secteurs public et privé par des points de terminaison sécurisés de services Web selon le schéma ci-dessous :

Figure II
Points de terminaison eTIR



14. Il convient de noter qu'il n'y a pour le moment qu'une seule chaîne de garantie en activité (à savoir l'Union internationale des transports routiers), mais que la Convention TIR ne limite pas le système à une seule chaîne de garantie.

B. Aperçu des messages de l'interface

15. Les messages eTIR sont classés en plusieurs catégories en interne, en fonction de l'expéditeur ou du destinataire du message et de la direction du message (le système eTIR étant au centre des échanges) :

- Tous les codes de messages commencent :
  - Par la lettre « I » pour les messages internes (internes au secteur public, c'est-à-dire entre le système international eTIR et les systèmes douaniers nationaux ou la Banque de données internationale TIR) ;
  - Par la lettre « E » pour les messages externes (externes au secteur public, c'est-à-dire entre le système international eTIR et une chaîne de garantie ou un titulaire de carnet TIR).
- Tous les messages vont par paire (demande-réponse), et leurs codes se terminent tous :
  - Par un nombre impair pour le message initial (appel ou demande) ;
  - Par un nombre pair pour le message en retour (accusé de réception ou réponse).

16. Voici la liste complète des messages internes et externes :

Messages externes	*Messages internes*
E1 − Enregistrer la garantie	**I1 − Accepter la garantie**
E2 − Résultats de l'enregistrement de la garantie	*I2 − Résultats de l'acceptation de la garantie*

Messages externes	*Messages internes*
E3 − Annuler la garantie	**I3 − Obtenir des informations sur le titulaire**
E4 − Résultats de l'annulation de la garantie	*I4 − Informations sur le titulaire*
E5 − Demander des informations sur la garantie	**I5 − Demander des informations sur la garantie**
E6 − Résultats de la demande d'informations sur la garantie	*I6 − Résultats de la demande d'informations sur la garantie*
E7 − Notifier la chaîne de garantie	**I7 − Enregistrer les données de la déclaration**
E8 − Confirmation de la notification à la chaîne de garantie	*I8 − Résultats de l'enregistrement des données de la déclaration*
E9 − Renseignements anticipés TIR	**I9 − Lancer l'opération TIR**
E10 − Résultats pour les renseignements anticipés TIR	*I10 − Résultats du lancement de l'opération TIR*
E11 − Renseignements anticipés rectifiés	**I11 − Achever l'opération TIR**
E12 − Résultats pour les renseignements anticipés rectifiés	*I12 − Résultats de l'achèvement de l'opération TIR*
E13 − Annuler les renseignements anticipés	**I13 − Apurer l'opération TIR**
E14 − Résultats de l'annulation des renseignements anticipés	*I14 − Résultats de l'apurement de l'opération TIR*
	I15 − Notifier les services douaniers
	I16 − Confirmation de la notification aux services douaniers
	I17 − Refuser le lancement d'une opération TIR
	I18 − Résultats du refus du lancement d'une opération TIR
	I19 − Vérifier les bureaux de douane
	I20 − Validation des bureaux de douane

17. Le système international eTIR vise à permettre l'échange sécurisé, entre les systèmes douaniers nationaux, de données relatives au transit international de marchandises, de véhicules ou de conteneurs sous couvert du régime TIR et à permettre aux services douaniers d'assurer la gestion des données sur les garanties émises par les chaînes de garantie aux titulaires de carnets TIR habilités.

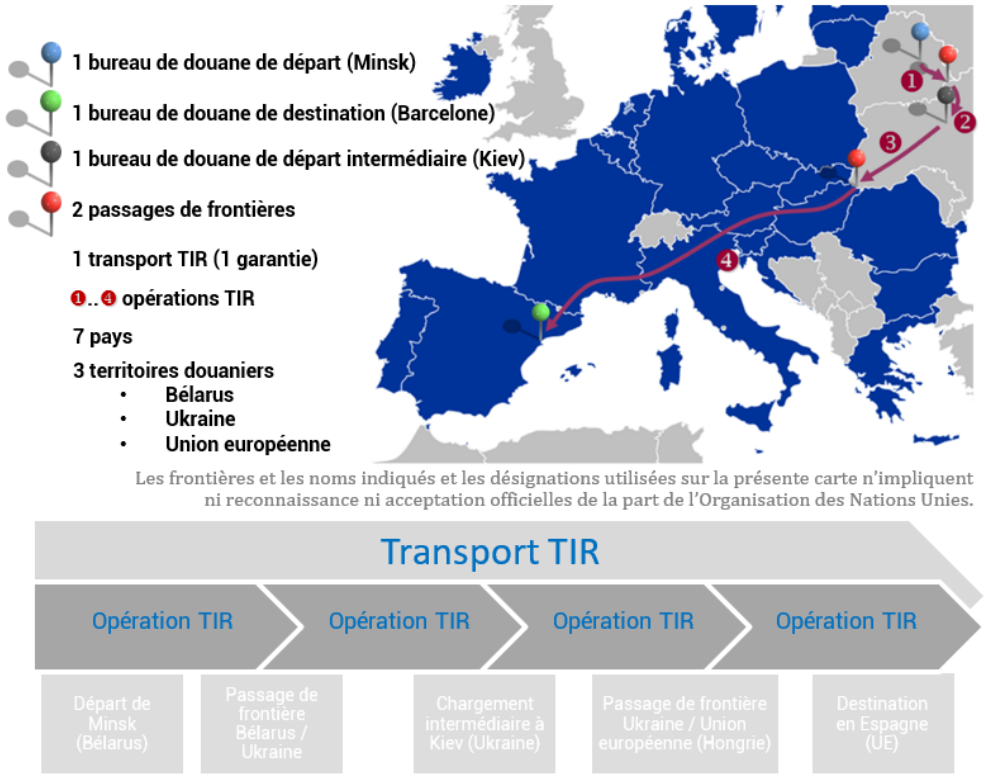
C. Transport TIR et opérations TIR dans le système eTIR

18. Le schéma ci-dessous met en évidence les concepts importants du transport TIR et des opérations TIR, et la figure qui lui succède donne un exemple de transport TIR :

Figure III
Résumé d'un transport TIR

19. Il importe de noter qu'un transport TIR peut comporter plusieurs points de chargement et de déchargement et, bien entendu, plusieurs passages de frontières. Chacun de ces événements sépare deux opérations TIR distinctes. Il convient également de préciser que les passages de frontière séparant des opérations TIR sont ceux qui s'effectuent entre deux territoires douaniers distincts (un territoire douanier pouvant être celui d'un pays ou celui d'une union douanière, comme dans le cas de l'Union européenne). On trouvera de plus amples détails à la page du Manuel eTIR consacrée à ce sujet[22].

Figure IV
Exemple de transport TIR



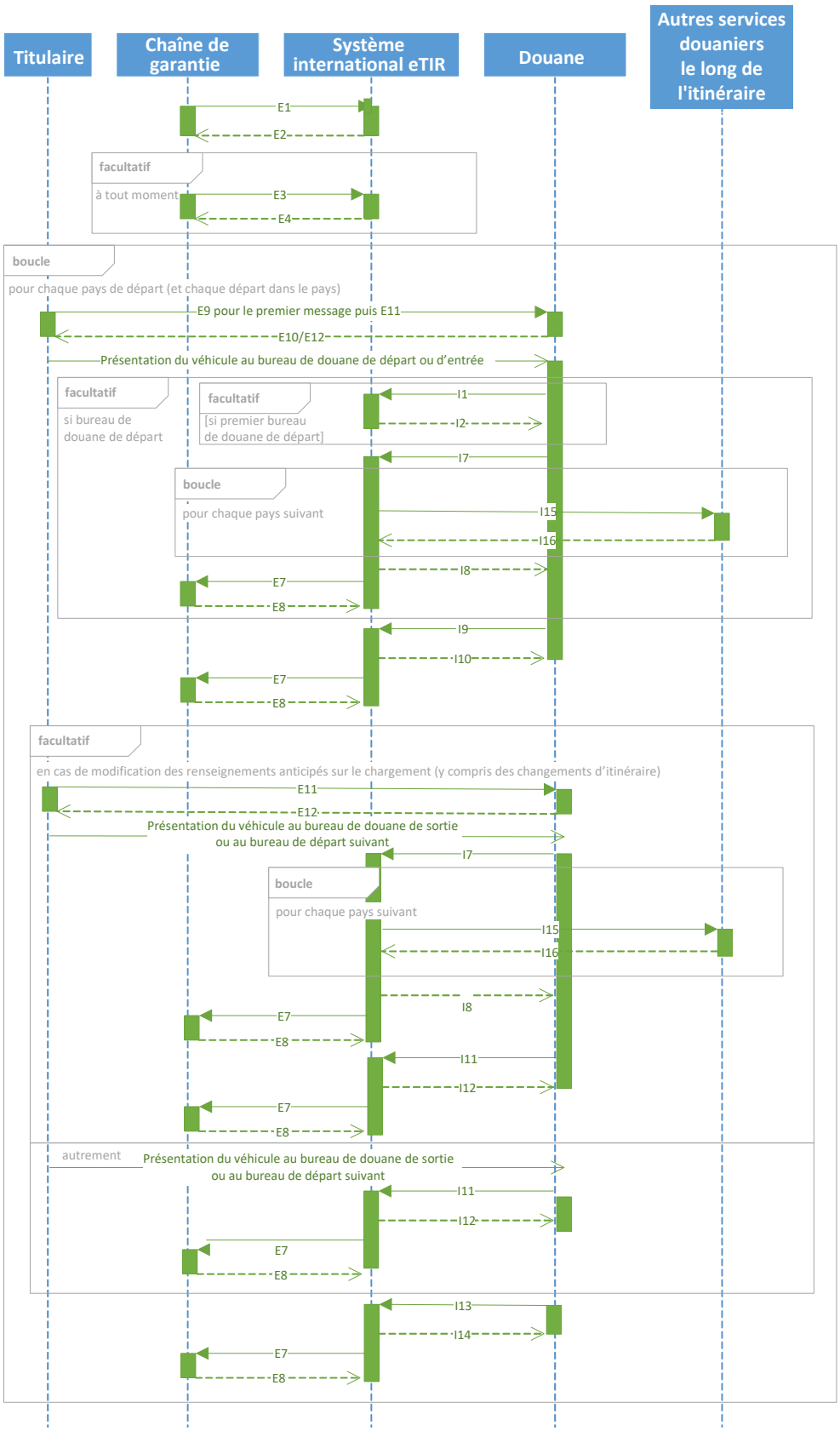
D. Diagrammes de séquence dans le système eTIR

20. L'utilisation des messages eTIR est décrite dans les diagrammes de séquence eTIR ci-dessous pour les pays de départ, de transit et de destination.

[22] https://unece.org/fileadmin/DAM/tir/handbook/french/newtirhand/TIR-6Rev11f.pdf#page=21.

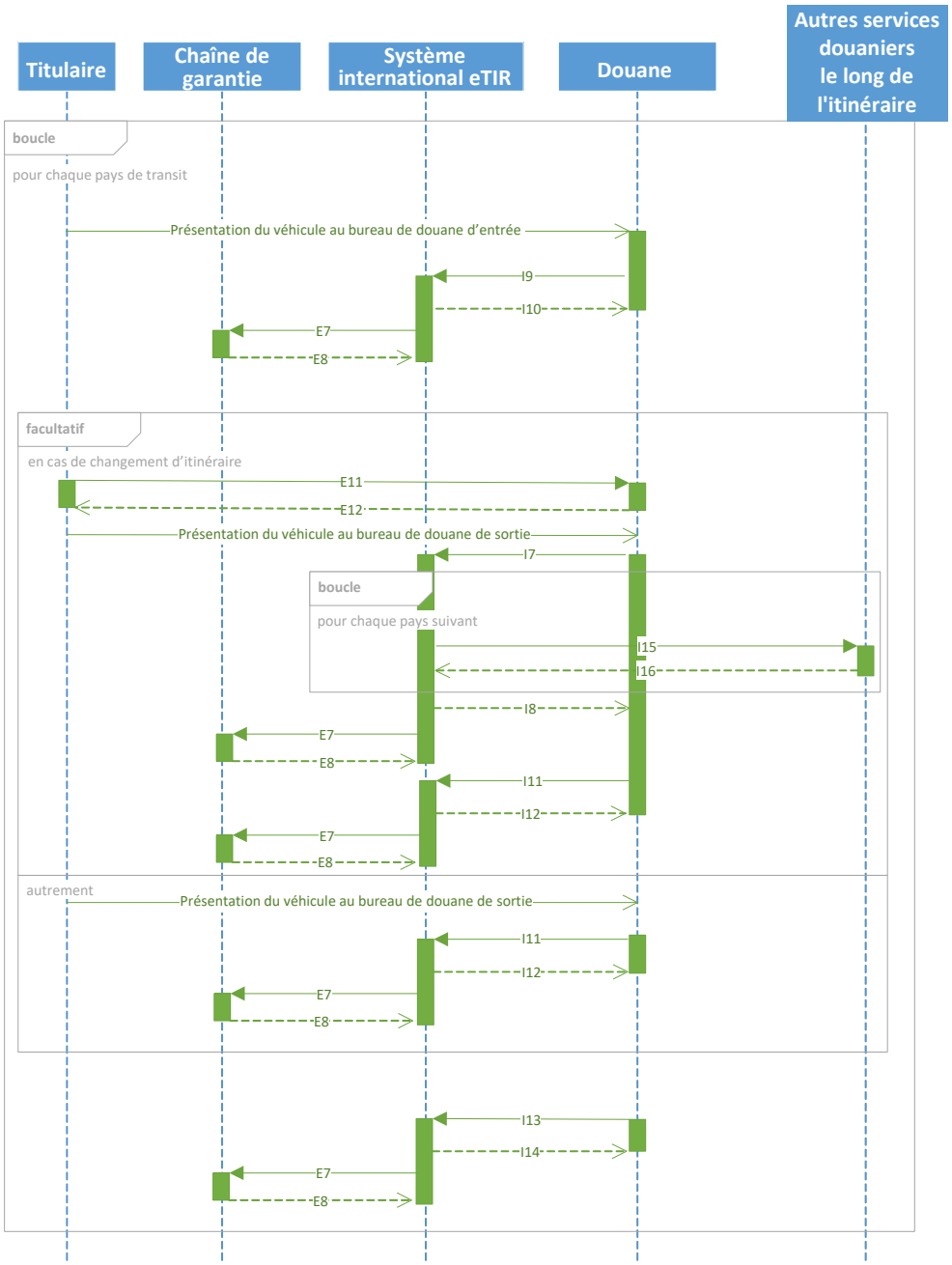
1. Séquence de messages pour les pays de départ

Figure V
Diagramme de séquence chronologique − pays de départ



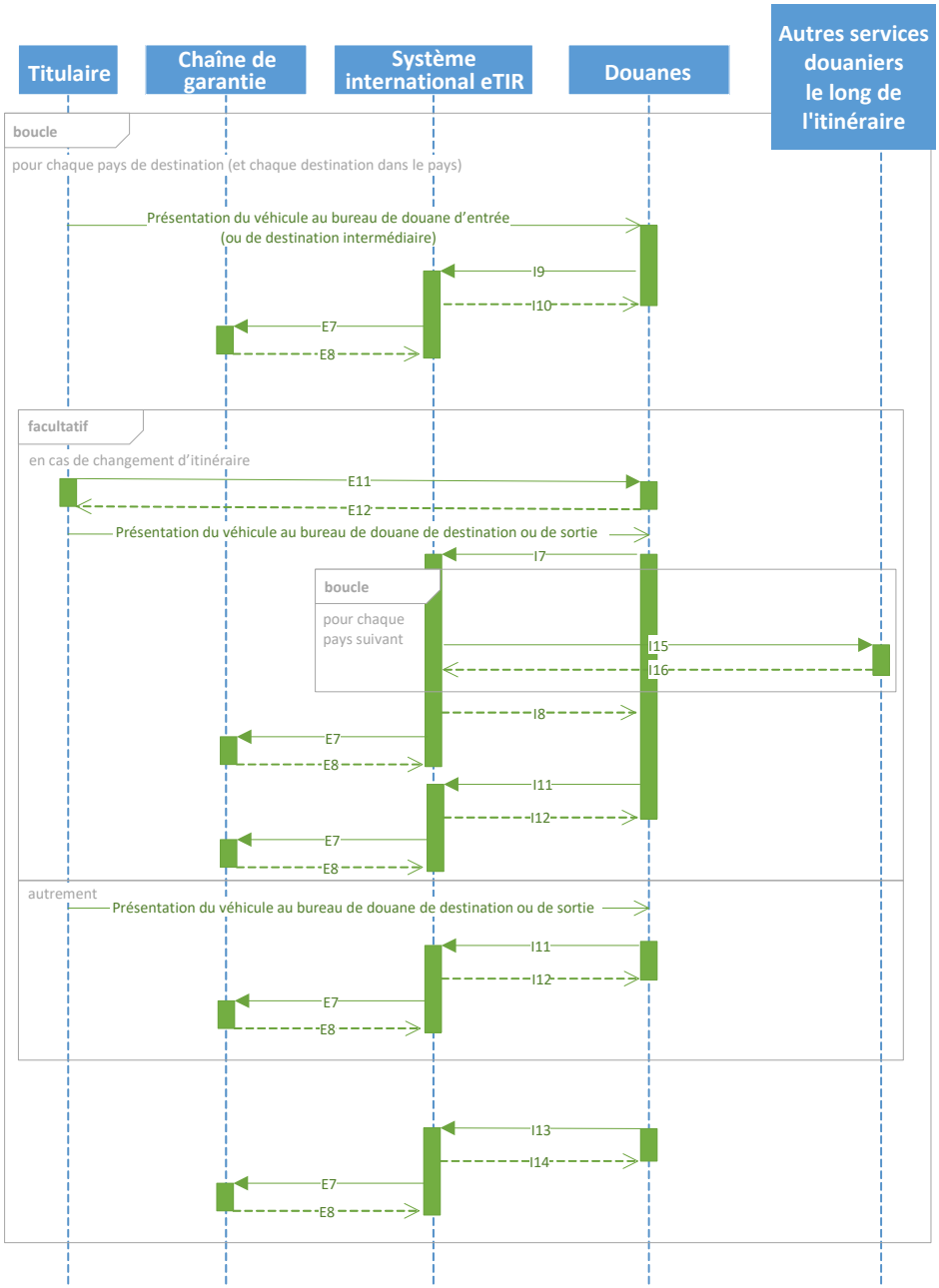
2. Séquence des messages pour les pays de transit

Figure VI
Diagramme de séquence chronologique − pays de transit



3. Séquence de messages pour les pays de destination

Figure VII
Diagramme de séquence chronologique − pays de destination



VII. Sécurité

21. Dans les services Web du système international eTIR, le protocole WS-Security est utilisé pour la signature électronique, mais pas pour le chiffrement des messages. Cette norme, qui existe depuis mars 2004, est unanimement reconnue et recommandée par le secteur des services Web.

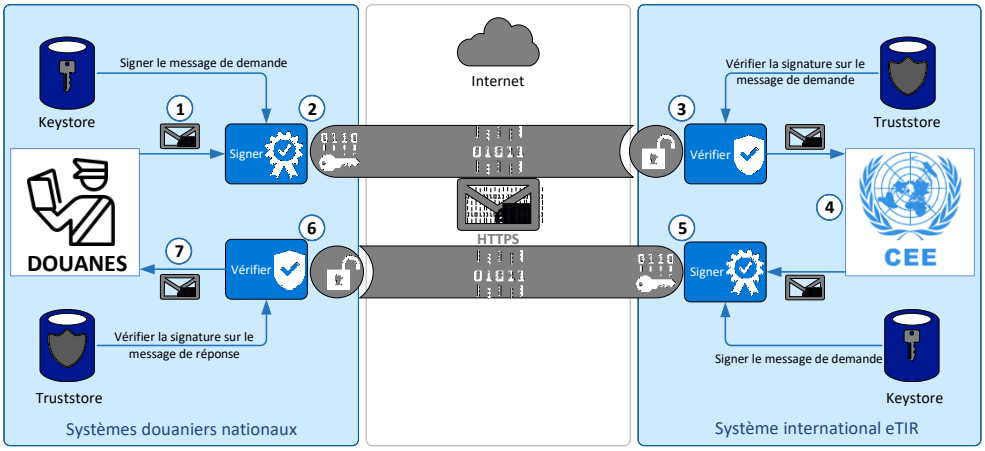
22. Une signature numérique reposant sur des certificats X.509 (version 3) sert à identifier l'émetteur d'un appel au service Web et permet la non-répudiation. Un protocole de chiffrement (TLS v1.2 ou v1.3) est utilisé pour l'envoi des messages par le protocole HTTPS afin de garantir la confidentialité des informations échangées dans les messages. Il convient de noter que des paires de clefs asymétriques différentes sont utilisées pour la signature numérique et le protocole de chiffrement (TLS).

23. Les termes et les notions relatifs à la sécurité des services Web utilisés dans l'ensemble du présent document sont décrits dans les paragraphes ci-dessous. Les termes « sécurité des services Web (WS-Security) », « jeton X.509 », « keystore » et « truststore », fréquemment employés, sont expliqués en détail dans le glossaire.

A. Modèle de sécurité du système eTIR

24. La figure ci-dessous représente le modèle WS-Security, dont un aperçu est présenté dans cette section pour illustrer le fonctionnement de ce modèle de sécurité.

Figure VIII
Modèle de sécurité du système eTIR



25. Il convient de noter que, si ce schéma correspond à la plupart des cas d'utilisation, il arrive parfois que le système international eTIR joue en réalité le rôle de client, et les systèmes douaniers nationaux celui de prestataire de services.

26. Dans l'exemple ci-dessus, avant tout, le certificat X.509 des systèmes douaniers nationaux est stocké dans le truststore du système international eTIR. De même, le certificat du système international eTIR est stocké dans le truststore des systèmes douaniers nationaux. Cette première étape obligatoire permet la validation des signatures numériques qui sont transférées comme jetons de sécurité dans tous les messages SOAP échangés dans le cadre de la procédure eTIR.

27. Voici comment une demande est envoyée par les systèmes douaniers nationaux au système international eTIR et comment la réponse correspondante est renvoyée :

a) Le système douanier national génère un message de demande à envoyer au service Web du système international eTIR ;

b) Le message de demande est signé avec la clef privée du certificat X.509 du système douanier national (stockée dans le keystore) et envoyé par le protocole HTTPS en utilisant un protocole de chiffrement (TLS) ;

c) Le système international eTIR reçoit le message de demande et en vérifie la signature à l'aide de la clef publique de l'expéditeur afin d'authentifier le message et d'en confirmer l'intégrité ;

d) Le système international eTIR traite le message de demande et génère un message de réponse en retour ;

e) Le message de réponse est signé avec la clef privée du système international eTIR (stockée dans le keystore) et envoyé par le protocole HTTPS en utilisant un protocole de chiffrement (TLS) ;

f) Le système douanier national reçoit le message de réponse et en vérifie la signature à l'aide de la clef publique du prestataire de services afin d'authentifier le message et d'en confirmer l'intégrité.

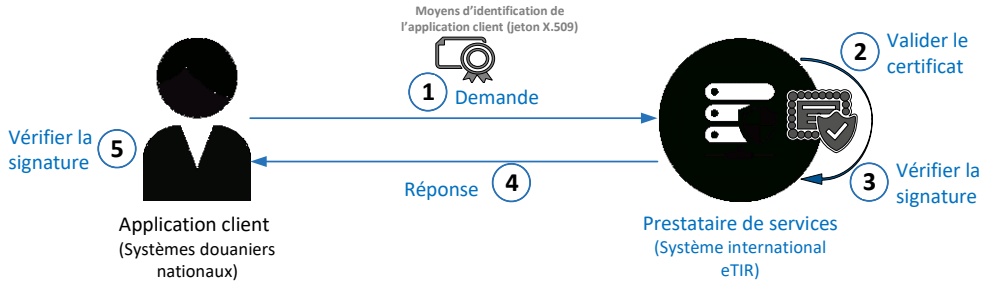
28. L'exécution de ce processus illustre l'application de quatre principes de sécurité que le système international eTIR entend concrétiser grâce à ce modèle de sécurité, à savoir l'authentification, l'intégrité, la confidentialité et la non-répudiation.

B. Authentification, intégrité et non-répudiation

29. L'authentification permet de garantir que les différentes parties à une transaction sont véritablement qui elles prétendent être, ce pourquoi elles doivent apporter la preuve de leur identité. Cette preuve peut être apportée de diverses manières. Par exemple, le plus simple est de fournir un identifiant d'utilisateur et le mot de passe secret correspondant. Une méthode plus sécurisée consiste à utiliser un certificat X.509 émis par une autorité de certification de confiance. Le certificat X.509 identifie l'utilisateur final. La clef privée du certificat X.509 sert également à signer les messages SOAP. Cette signature électronique permet de garantir non seulement l'identité de l'expéditeur, mais aussi l'intégrité du message, c'est-à-dire le fait que son contenu n'a pas été modifié au cours de la transmission. L'expéditeur utilise sa clef privée pour signer le message (la valeur de hachage du message, plus précisément), et le destinataire utilise la clef publique de l'expéditeur pour vérifier la signature ; la non-répudiation est ainsi établie.

1. Étapes de l'authentification à l'aide d'un certificat X.509

Figure IX
Étapes de l'authentification



- L'application client (système douanier national) envoie un message au prestataire de services (système international eTIR) (étape 1). Le message contient les moyens d'identification de l'application client, signés à l'aide de la clef privée associée à la clef publique figurant dans le certificat X.509 de l'application client. Le prestataire de services valide le certificat en procédant aux contrôles énumérés aux points suivants (étape 2) :
    - Il vérifie que le certificat n'a pas expiré : si la date d'expiration du certificat est échue, ce certificat n'est plus valable.
    - Il vérifie que le certificat est intrinsèquement cohérent : le service contrôle que les données du certificat n'ont pas été modifiées en comparant le contenu du certificat et la signature de l'autorité de certification émettrice.
    - Il vérifie l'autorité de certification ayant délivré le certificat X.509 du client : pour ce faire, le service compare la signature de l'émetteur sur le certificat X.509 de l'application client avec le certificat X.509 de l'autorité de certification émettrice. Pour que cette étape s'effectue correctement, l'autorité de certification ayant délivré le certificat X.509 du client doit être reconnue par l'application client et par le prestataire de services.
    - Il vérifie que l'autorité de certification émettrice n'a pas annulé le certificat : le prestataire de services contrôle que le certificat X.509 ne figure pas sur une liste des annulations de certificats publiée par l'autorité de certification émettrice. Le service peut contrôler si le certificat a été annulé soit en y accédant directement auprès de l'autorité de certification, soit en vérifiant

dans une liste des annulations de certificats téléchargée au préalable auprès de l'autorité de certification émettrice et enregistrée dans le registre des certificats que le service utilise pour rechercher les certificats X.509.

- Enfin, le prestataire de services utilise la clef publique du certificat X.509 de l'application client pour vérifier la signature de l'application client (étape 3). Cette méthode permet au prestataire de services d'authentifier l'application client et de s'assurer que les données signées n'ont pas été modifiées après la signature du message.

30. En cas d'échec de l'authentification, le prestataire de services renvoie le message d'erreur HTTP 500. Si l'authentification réussit, il traite le contenu de la demande et génère le message de réponse prévu dans les spécifications eTIR (étape 4). À réception du message de réponse, l'application client devra également effectuer les contrôles décrits ci-dessus (étape 5).

2. Génération de paires de clefs

31. Les administrations douanières peuvent obtenir une paire de clefs publique-privée auprès d'une autorité de certification de confiance ou créer des certificats autosignés. Elles doivent générer une paire de clefs RSA, transmettre à l'équipe du secrétariat TIR de la CEE la partie publique (certificat X.509) de la clef générée et conserver la clef privée sous haute protection dans leur keystore. Il existe deux manières possibles de générer une paire de clefs RSA, qui sont décrites dans les annexes.

C. Confidentialité

32. Le protocole de transfert hypertexte sécurisé (HTTPS), utilisé pour accéder aux points de terminaison du système international eTIR, est une extension du protocole de transfert hypertexte (HTTP) dans laquelle la communication est chiffrée au moyen du protocole de chiffrement TLS (Transport Layer Security), conçu pour assurer la sécurité des communications sur les réseaux publics tels qu'Internet. La principale raison justifiant l'utilisation du protocole HTTPS est la nécessité de garantir la confidentialité et l'intégrité des données échangées pendant la transmission. Ce protocole protège contre les menaces visant la sécurité des informations, par exemple une attaque de de type « homme du milieu ». Le chiffrement bidirectionnel des communications entre un client et un serveur permet d'éviter que les données échangées soient interceptées et modifiées. Ainsi, les communications entre le système international eTIR et les systèmes douaniers nationaux sont sécurisées grâce au chiffrement bidirectionnel au moyen du protocole TLS (v1.2 au minimum).

VIII. Accès aux services Web eTIR

A. Conditions préalables

1. Réseaux

33. Les systèmes douaniers nationaux doivent avoir accès à Internet, et tous les domaines des environnements d'essais d'acceptation et d'exploitation décrits ci-après doivent être approuvés (liste blanche) par les ingénieurs réseau des autorités douanières. Par ailleurs, dans le cadre du système international eTIR, le protocole SOAP est mis en œuvre pour utiliser le protocole HTTPS sur le port TCP/8083 ; ce protocole et ce port doivent donc être ouverts dans les pare-feu des autorités douanières pour que les systèmes douaniers nationaux puissent les utiliser.

2. Certificats

34. Comme expliqué dans la section relative à la sécurité, pour que la connexion entre le système international eTIR et les systèmes douaniers nationaux soit possible il faut que les deux parties échangent leurs certificats X.509 et les stockent mutuellement dans leur truststore.

35. Cette procédure doit être effectuée pour chaque paire d'environnement client-service au cours de la phase de mise en œuvre. Cela signifie que l'environnement d'essais d'acceptation de chaque système douanier national doit être connecté à l'environnement d'essais d'acceptation du système international eTIR. Une fois prêts, les environnements d'exploitation des deux parties doivent échanger leurs certificats X.509 d'exploitation afin de permettre la communication entre eux et l'utilisation de la procédure eTIR dès que le lancement sera confirmé.

36. Les deux systèmes (le système international eTIR et les systèmes douaniers nationaux) doivent utiliser des certificats X.509 différents pour leur environnement d'essais d'acceptation et pour leur environnement d'exploitation. Il convient également de noter que, bien que le présent document fasse référence à des méthodes permettant de générer localement des certificats à l'aide d'un logiciel libre qui peuvent être utiles à des fins d'essai et de mise au point, l'équipe informatique de chaque administration douanière est entièrement libre de choisir les certificats qu'elle génère et échange, à condition que ceux-ci respectent les prescriptions et les consignes de sécurité prescrites dans le présent document.

37. Outre le certificat X.509 généré, le certificat du serveur de la CEE (unece.org.cer) sera utilisé dans le mécanisme de chiffrement (HTTPS) du message. Selon le cas, il pourra être nécessaire de l'extraire pour le stocker dans le truststore, si l'application ne le fait pas automatiquement (option à privilégier).

38. Au cours du processus de génération de certificat expliqué dans la section « Keystore : explication pas à pas pour la génération de paires de clefs », le champ de l'adresse électronique doit être correctement rempli, car cette adresse sera utilisée par le système international eTIR pour l'envoi de notifications.

3. Inscription des serveurs sur la liste blanche

39. Pour que les serveurs des systèmes douaniers nationaux puissent se connecter au système international eTIR, ils doivent d'abord être inscrits sur une liste blanche par l'équipe de sécurité informatique de la CEE. À cette fin, les experts informatiques des autorités douanières doivent communiquer au secrétariat TIR toutes les adresses IP des serveurs de leur système douanier national qui enverront des demandes au système international eTIR. De même, le secrétariat TIR se tient prêt à leur transmettre les adresses IP des serveurs de la CEE afin que la même opération soit effectuée du côté des autorités douanières.

B. Adresses URL des environnements d'essais et d'exploitation

40. La liste ci-dessous fournit les informations sur les points de terminaison des services Web pour les environnements d'exploitation et d'essais d'acceptation, ainsi que les adresses URL correspondantes pour les fichiers en langage de description des services Web (WSDL) :

- URL de base des services Web dans l'environnement d'essais d'acceptation :

  etir-uat-01.unece.org/etir/v4.3/customs

- Fichier WSDL pour les autorités douanières :

  etir-uat-01.unece.org/etir/v4.3/customs?wsdl

- Fichier WSDL pour les chaînes de garantie :

  etir-uat-01.unece.org/etir/v4.3/guaranteeChain?wsdl

IX. Mise en œuvre et mise à l'essai des messages eTIR

A. Approche générale recommandée

1. Objet

41. Dans la présente section, le secrétariat TIR souhaite faire part de la méthode qu'il a appliquée pour mettre en œuvre le système international eTIR dans les délais et dans le

respect de la qualité. Il souhaite ainsi faire profiter le lecteur des enseignements tirés de cette expérience.

2. Approche générale

42. Le secrétariat TIR a adopté une méthode dite « Agile » obéissant aux principes du manifeste du même nom. L'équipe informatique se réunit toutes les semaines pour passer en revue le travail accompli au cours de la semaine précédente, discuter des tâches à effectuer pendant la semaine en cours et faire état de tout obstacle éventuel que les autres membres de l'équipe pourraient aider à contourner. Dans ses travaux, le secrétariat TIR s'appuie sur un système interne de gestion des connaissances comprenant :

- Un système de suivi des problèmes permettant de gérer toutes les tâches à effectuer, qui offre les meilleures garanties en matière de traçabilité et de responsabilisation ;
- Une plateforme qui héberge toute la documentation relative à la mise au point, à la gestion et à l'exploitation du projet eTIR ;
- Un système de gestion du code source qui héberge les dépôts de code des systèmes informatiques TIR.

3. Intégration continue

43. Le secrétariat TIR a également adopté les meilleures pratiques de la communauté DevOps. En particulier, il reconnaît à quel point il est important et utile d'automatiser le plus possible de processus au cours du cycle de développement d'un logiciel afin de soulager les humains de tâches sans intérêt, d'améliorer la fiabilité en réduisant la probabilité d'erreurs humaines et d'accroître considérablement la productivité.

44. Pour optimiser la fiabilité du système, le nouveau code est régulièrement déployé dans le cadre d'un processus d'intégration continue. De plus, le code de base est intégralement reconstruit chaque fois que du nouveau code est ajouté dans le dépôt de code, de sorte que toutes les fonctionnalités achevées fonctionnent comme prévu en permanence.

4. Essais approfondis

45. Un outil d'analyse de code statique est utilisé pour vérifier tous les jours le code source par rapport à des ensembles de règles et de meilleures pratiques créées par la communauté du secteur informatique, ce qui permet de garantir une qualité élevée du code source et contribue à la formation continue des membres de l'équipe informatique.

46. L'objectif est que 70 % du code de base fonctionnel soient soumis à des essais unitaires, ainsi qu'à une série complète d'essais fonctionnels de non-régression élaborés en collaboration avec Apache JMeter. La combinaison de ces deux types d'essais permet de contrôler le bon fonctionnement de chaque partie du système international eTIR et de se protéger contre d'éventuelles régressions lors de l'ajout de nouveau code au code de base.

B. Trousse à outils : liste des logiciels jugés utiles

47. Les divers logiciels énumérés ci-dessous sont ceux qui sont jugés utiles pour le déploiement d'une application client connectée au système international eTIR et que le secrétariat TIR a déjà expérimentés :

- Suite de tests SoapUI : un logiciel utile pour effectuer des tests ponctuels sur les messages SOAP (le mini-guide SoapUI est fourni en annexe) ;
- Suite de tests JMeter : un logiciel utile pour automatiser les tests des messages et couvrir un large éventail de scénarios ;
- Système de gestion de version GIT : le gestionnaire de version le plus répandu dans le secteur, qui permet de contrôler que la bonne version est utilisée pour tout le code du système international eTIR et les autres éléments de configuration ;

- IntelliJ IDEA : l'un des principaux environnements de développement intégrés, regroupant les outils techniques de développement du système international eTIR, qui a contribué à l'amélioration de la productivité sur divers aspects ;
- Outil d'analyse statique de code SonarQube : un logiciel utilisé pour le contrôle en continu de la qualité du code, qui effectue des examens automatiques avec une analyse statique du code pour détecter les bogues, les « code smells » (c'est-à-dire les signes de mauvaises pratiques de codage) et les failles de sécurité.

48. Il convient de noter qu'il n'est pas obligatoire d'installer ou d'utiliser ces applications. Toutefois, ces outils ont fait leurs preuves et le secrétariat TIR les a trouvés utiles pendant la mise en œuvre du système international eTIR.

C. Génération de l'en-tête de sécurité dans les messages SOAP

49. Le système international eTIR s'appuie sur un échange de messages Web au moyen du protocole SOAP v1.2. WS-Security, une extension du protocole SOAP, fournit l'élément d'en-tête SOAP intitulé « Security », qui est conçu pour servir de conteneur destiné à stocker toutes les informations relatives à la sécurité pour les messages SOAP de demande et de réponse. La présente section explique comment l'élément **Security** est défini dans le schéma WS-Security.

1. Éléments de l'en-tête Security

50. L'en-tête wsse:Security est un mécanisme permettant d'incorporer des informations relatives à la sécurité s'adressant à un destinataire particulier désigné sous la forme d'un acteur ou d'un rôle SOAP. Cet élément représente les étapes de signature que le producteur du message a suivies pour créer le message. Grâce à cette règle consistant à joindre ces informations avant le corps du message (préfixe), l'application destinataire peut traiter les sous-éléments dans l'ordre où ils apparaissent dans l'en-tête wsse:Security, car ils ne dépendent d'aucun élément apparaissant plus loin dans le message.

Élément Signature

L'élément **Signature** est l'élément racine d'une signature XML.

Définition de schéma

```
<element name="Signature" type="ds:SignatureType"/>
  <complexType name="SignatureType">
    <sequence>
      <element ref="ds:SignedInfo"/>
      <element ref="ds:SignatureValue"/>
      <element ref="ds:KeyInfo" minOccurs="0"/>
      <element ref="ds:Object" minOccurs="0" maxOccurs="unbounded"/>
    </sequence>
    <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

Exemple dans un message

```
<ds:Signature Id="SIG-AD473EF9595256C9D115409733594021 73"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces PrefixList="SOAP-ENV cus urn"
              xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:CanonicalizationMethod>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <ds:Reference URI="#id-AD473EF9595256C9D115409733594011 72">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                <ec:InclusiveNamespaces PrefixList="cus urn"
                  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
              </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>H2Ai…</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>bY65hsJdkxh40…
        </ds:SignatureValue>
        <ds:KeyInfo Id="KI-AD473EF9595256C9D115409733594011 70">
          <wsse:SecurityTokenReference wsu:Id="STR-AD473EF9595256C9D115409733594011 71">
            <wsse:KeyIdentifier EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-1.0#Base64Binary"
                                ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
profile-1.0#X509v3">
              G9w0BAQsFAAN...
            </wsse:KeyIdentifier>
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
      </ds:Signature>
```

Élément SignatureValue

51. L'élément SignatureValue contient les informations relatives à la clef publique de l'expéditeur qui sont nécessaires pour que le système international eTIR puisse valider la signature numérique de l'émetteur de l'appel. Il est toujours encodé en base64.

Définition de schéma

```
<element name="SignatureValue" type="ds:SignatureValueType" />

  <complexType name="SignatureValueType">
    <simpleContent>
      <extension base="base64Binary">
        <attribute name="Id" type="ID" use="optional"/>
      </extension>
    </simpleContent>
  </complexType>
```

Exemple dans un message

```
<ds:SignatureValue>
    bY65hsJdkxh40…
</ds:SignatureValue>
```

52. L'élément SignatureValue contient une signature qui ne couvre que l'élément SignedInfo : seul le contenu de cet élément SignedInfo est inclus dans le résumé de la signature.

Élément SignedInfo

53. L'élément SignedInfo indique quelle partie du message a été utilisée pour générer la signature. Il comporte un attribut Id qui renvoie à la partie du corps du message SOAP signé ; ce point sera expliqué plus en détail dans le prochain élément (Reference). La structure de l'élément SignedInfo se compose de l'algorithme de canonisation, d'un algorithme de signature et d'une ou plusieurs références. Le contenu de l'élément SignedInfo peut se diviser en deux parties : des informations sur l'élément SignatureValue et des informations sur le contenu de l'application, comme le montre le fragment de schéma XML ci-dessous :

Définition de schéma

```
<element name="SignedInfo" type="ds:SignedInfoType"/>

  <complexType name="SignedInfoType">
    <sequence>
      <element ref="ds:CanonicalizationMethod"/>
      <element ref="ds:SignatureMethod"/>
      <element ref="ds:Reference" maxOccurs="unbounded"/>
    </sequence>
    <attribute name="Id" type="ID" use="optional"/>
  </complexType>
```

Exemple dans un message

```
<ds:SignedInfo>
  <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
    <ec:InclusiveNamespaces PrefixList="SOAP-ENV cus urn"
      xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </ds:CanonicalizationMethod>
  <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
  <ds:Reference URI="#id-AD473EF9595256C9D11540973359401172">
    <ds:Transforms>
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
        <ec:InclusiveNamespaces PrefixList="cus urn"
          xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transform>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>H2Ai⋯</ds:DigestValue>
  </ds:Reference>
</ds:SignedInfo>
```

54. La canonisation, ou C14N (canonisation XML exclusive), est le processus consistant à choisir un chemin parmi toutes les options de sortie possibles pour que l'expéditeur et le destinataire puissent générer exactement la même valeur d'octet, quel que soit le logiciel XML intermédiaire utilisé. L'élément SignedInfo/CanonicalizationMethod indique comment reconstruire le flux d'octets exact. L'élément SignedInfo/SignatureMethod spécifie le type d'algorithme (par exemple, Kerberos ou RSA) utilisé pour générer la signature. Ensemble, ces deux éléments décrivent comment créer le résumé et comment le protéger contre toute modification.

55. Dans une application client en Java, cela peut être configuré comme suit :

```
org.apache.wss4j.dom.message.WSSecSignature wsSecSignature = new WSSecSignature();
//http://www.w3.org/2001/10/xml-exc-c14n#
wsSecSignature.setSigCanonicalization(WSConstants.C14N_EXCL_OMIT_COMMENTS);
//http://www.w3.org/2000/09/xmldsig#rsa-sha1
wsSecSignature.setSignatureAlgorithm(WSConstants.RSA_SHA1);
```

Élément Reference

56. L'élément Reference sert à renvoyer vers un autre contenu. Il contient un résumé du contenu, une description de la méthode utilisée pour générer ce résumé (par exemple, SHA1) et une spécification concernant la manière dont le contenu doit être transformé avant que le résumé soit généré. Les transformations procurent de la souplesse quant à la construction de la signature XML.

Définition de schéma

```
<element name="Reference" type="ds:ReferenceType"/>

  <complexType name="ReferenceType">
    <sequence>
      <element ref="ds:Transforms" minOccurs="0"/>
      <element ref="ds:DigestMethod"/>
      <element ref="ds:DigestValue"/>
    </sequence>
    <attribute name="Id" type="ID" use="optional"/>
    <attribute name="URI" type="anyURI" use="optional"/>
    <attribute name="Type" type="anyURI" use="optional"/>
  </complexType>
```

Exemple dans un message

```
<ds:Reference URI="#id-AD473EF9595256C9D11540973359401172">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
      <ec:InclusiveNamespaces PrefixList="cus urn"
        xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    </ds:Transform>
  </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <ds:DigestValue>H2Ai…</ds:DigestValue>
</ds:Reference>
```

57. L'élément DigestMethod spécifie l'algorithme de hachage, et l'élément DigestValue correspond à la valeur de hachage du contenu encodé en base64. Le principal composant de l'élément Reference est l'ensemble des transformations pouvant être utilisées. L'élément Transforms contient une liste des éléments Transform, dont chacun correspond à une étape de transformation.

Élément Transforms

58. Le schéma définit un éventail de transformations, dont un élément XPath qui a une structure définie :

Définition de schéma

```
<element name="Transforms" type="ds:TransformsType"/>
  <complexType name="TransformsType">
    <sequence>
      <element ref="ds:Transform" maxOccurs="unbounded"/>
    </sequence>
  </complexType>

<element name="Transform" type="ds:TransformType"/>
  <complexType name="TransformType" mixed="true">
    <choice minOccurs="0" maxOccurs="unbounded">
      <any namespace="##other" processContents="lax"/>
      <element name="XPath" type="string"/>
    </choice>
    <attribute name="Algorithm" type="anyURI" use="required"/>
  </complexType>
```

59. Le contenu d'un élément Transform dépendra de l'attribut Algorithm. Par exemple, si du XML simple est signé, alors il y aura très probablement un seul élément Transform indiquant un algorithme C14N :

Exemple dans un message

```
<ds:Transforms>
  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
    <ec:InclusiveNamespaces PrefixList="cus urn"
      xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </ds:Transform>
</ds:Transforms>
```

Élément KeyInfo

60. La dernière étape consiste à identifier le signataire, ou au moins la clef qui a généré la signature (la clef qui empêche de modifier le résumé). C'est l'élément KeyInfo qui remplit cette fonction :

Définition de schéma

```
<element name="KeyInfo" type="ds:KeyInfoType"/>

  <complexType name="KeyInfoType" mixed="true">
    <choice maxOccurs="unbounded">
      <element ref="ds:KeyName"/>
      <element ref="ds:KeyValue"/>
      <element ref="ds:RetrievalMethod"/>
      <element ref="ds:X509Data"/>
      <element ref="ds:PGPData"/>
      <element ref="ds:SPKIData"/>
      <element ref="ds:MgmtData"/>
      <any processContents="lax" namespace="##other"/>
    </choice>
    <attribute name="Id" type="ID" use="optional"/>
  </complexType>
```

Exemple dans un message

```
<ds:KeyInfo Id="KI-AD473EF9595256C9D11540973359401170">
  <wsse:SecurityTokenReference wsu:Id="STR-AD473EF9595256C9D11540973359401171">
    <wsse:KeyIdentifier EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary"
                        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3">
              G9w0BAQsFAAN...
    </wsse:KeyIdentifier>
  </wsse:SecurityTokenReference>
</ds:KeyInfo>
```

Élément SecurityTokenReference

61. L'opération de signature numérique nécessite qu'une clef soit indiquée. L'élément contenant la clef en question peut se trouver ailleurs dans le message ou complètement en dehors du message. L'élément SecurityTokenReference est un mécanisme qui permet, selon un modèle de contenu libre, de répertorier les jetons de sécurité et les autres éléments contenant des clefs. Il doit contenir soit un élément KeyIdentifier soit un élément X509Data. Si les configurations KeyIdentifier par défaut ne sont pas spécifiées, l'élément wsse:SecurityTokenReference contiendra un élément X509Data. Les deux options sont acceptées.

62. La configuration suivante permet de définir l'élément KeyIdentifier au lieu d'utiliser un élément X509Data :

```
org.apache.wss4j.dom.message.WSSecSignature wsSecSignature = new WSSecSignature();
wsSecSignature.setKeyIdentifierType(WSConstants.X509_KEY_IDENTIFIER);
```

Élément KeyIdentifier

63. Il convient d'utiliser un élément KeyIdentifier pour renvoyer à un jeton. Le tableau ci-dessous indique le codage et les types de valeur.

Fragment URI	URL
#Base64Binary	*http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary*
#X509v3	*http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3*

Exemple dans un message

```
<ds:KeyInfo Id="KI-AD473EF9595256C9D11540973359401170">
  <wsse:SecurityTokenReference wsu:Id="STR-AD473EF9595256C9D11540973359401171">
    <wsse:KeyIdentifier EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary"
                        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3">
        G9w0BAQsFAAN...
    </wsse:KeyIdentifier>
  </wsse:SecurityTokenReference>
</ds:KeyInfo>
```

Élément X509Data

Définition de schéma

```
<complexType name="X509IssuerSerialType">
  <sequence>
    <element name="X509IssuerName" type="string"/>
    <element name="X509SerialNumber" type="integer"/>
  </sequence>
</complexType>
```

64. Les certificats X.509 sont pris en charge au moyen de l'élément ds:X509Data. Cet élément permet au signataire d'intégrer son certificat (encodé en base64) ou toute autre méthode de vérification du certificat : un nom de sujet, le nom de l'émetteur et le numéro de série, l'identifiant de la clef ou un autre format. Le signataire peut également inclure une copie à jour de la liste des annulations de certificats, afin de démontrer que son identité était valable au moment où le document a été signé.

2. Exemple de message SOAP dans le système eTIR

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:cus="etir:v4.3:customs" xmlns:etir=
"etir:I5:v4.3">
  <soap:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
      xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
      <ds:Signature Id="SIG-AD473EF9595256C9D11540973359402173"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces PrefixList="soap wsa cus etir"
              xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:CanonicalizationMethod>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <ds:Reference URI="#id-AD473EF9595256C9D11540973359401172">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                <ec:InclusiveNamespaces PrefixList="cus etir"
                  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
              </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>H2Ai···</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>bY65hsJdkxh40···
        </ds:SignatureValue>
        <ds:KeyInfo Id="KI-AD473EF9595256C9D11540973359401170">
          <wsse:SecurityTokenReference wsu:Id="STR-AD473EF9595256C9D11540973359401171">
            <wsse:KeyIdentifier EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3">
              G9w0BAQsFAAN...
            </wsse:KeyIdentifier>
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
      </ds:Signature>
    </wsse:Security>
    <wsa:Action>etir:v4.3:customs/queryGuarantee</wsa:Action>
    <wsa:MessageID>uuid:8a20af11-8170-495d-9563-6a89b32ef745</wsa:MessageID>
  </soap:Header>
  <soap:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id=
"id-942cd702-1de3-4f27-bfcd-6628ab5d3143">
    <cus:queryGuarantee>
      <etir:InterGov>
        <etir:FunctionCode>9</etir:FunctionCode>
        <etir:ID>656dbce8-e810-44ec-8f3d-5f8a9b425d99</etir:ID>
        <etir:TypeCode>I5</etir:TypeCode>
        <etir:ReplyTypeCode>00</etir:ReplyTypeCode>
        <etir:ObligationGuarantee>
          <etir:ReferenceID>XC95xxxxxx</etir:ReferenceID>
        </etir:ObligationGuarantee>
      </etir:InterGov>
    </cus:queryGuarantee>
  </soap:Body>
</soap:Envelope>
```

D. Utilisation des champs Identifiant message et Référence fonctionnelle

1. Généralités

65. Tous les messages envoyés et reçus sont identifiés à l'aide du champ Identifiant message (Message Identifier). Ce champ doit être rempli par l'expéditeur dans le message de demande. Le destinataire définira une autre valeur unique pour le champ Identifiant message dans le message de réponse. En outre, le destinataire remplira également le champ Référence fonctionnelle (Functional Reference) dans le message de réponse en y indiquant la valeur du champ Identifiant message qui figure dans le message de demande correspondant. Cette méthode permet une traçabilité complète des messages de demande et de réponse.

2. Message de demande

66. Le destinataire doit définir le champ Identifiant message selon le format suivant :

```
SenderID:UUID
```

67. Où :

- SenderID est une valeur unique identifiant l'expéditeur. Cette valeur doit être identique à celle indiquée dans le champ d'identification de l'expéditeur dans le message.
- UUID est un identifiant unique universel de version 4 comme indiqué dans la RFC 4122. La version 4 est basée sur des chiffres pseudo-aléatoires, d'où la nécessité de conserver l'identifiant de l'expéditeur (SenderID) afin de diminuer les probabilités de collisions entre des messages envoyés par différents acteurs du système eTIR.

68. Les principaux langages de programmation fournissent des classes d'aide natives permettant de générer un UUID v4 :

En Java :

```
java.util.UUID.randomUUID();
```

En C# :

```
System.Guid.NewGuid();
```

69. Voici quelques exemples de valeurs valables pour le champ **Identifiant message** :

Exemple 1 :

```
<urn:ID>CustomsCountryA:6aca5f82-2285-4f00-b4ae-36269d4cc865</urn:ID>
```

Exemple 2 :

```
<urn:ID>eTIRInternationalSystem:1486e5b7-c6ae-4d27-b794-44c4bf545fb3</urn:ID>
```

3. Message de réponse

70. Le destinataire reçoit le message de demande de l'expéditeur et enregistre la valeur du champ Identifiant message. Lorsqu'il préparera le message de réponse, le destinataire définira une nouvelle valeur pour le champ Identifiant message, de la même manière que ci-dessus. La valeur enregistrée du champ Identifiant message dans le message de demande sera ensuite reportée dans le champ Référence fonctionnelle du message de réponse.

E. Utilisation des champs de date

71. Les messages eTIR comportent plusieurs champs dans lesquels il faut entrer des dates. Pour certains de ces champs, le format n'inclut que la date et, pour d'autres, il contient aussi l'heure. Cette section explique plus en détail comment remplir correctement ces champs.

1. Champs comprenant uniquement une date

72. Dans les fichiers XSD (XML Schema Definition), ce type de champ est nommé EtirDateType, et il est défini comme suit, avec les types dont il hérite :

Définition du type EtirDateType

```
<xs:complexType name="EtirDateType">
  <xs:simpleContent>
    <xs:extension base="ds:DateTimeType_102_S">
      <xs:attribute name="formatCode" use="optional">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="102"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:simpleType name="DateTimeType_102_S">
  <xs:restriction base="ds:DateTimeType_S">
    <xs:pattern value="[1-9][0-9][0-9][0-9](([0][1|3|5|7|8])([0][1-9]|[1-2][0-9]|[3][0-1])|([0][4|6|9])([0][1-9]|[1-
2][0-9]|[3][0])|([0][2])([0][1-9]|[1-2][0-9])|([1][0|2])([0][1-9]|[1-2][0-9]|[3][0-1])|([1][1])([0][1-9]|[1-2][0-
9]|[3][0]))"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="DateTimeType_S">
  <xs:restriction base="xs:string">
    <xs:pattern value=".{1,35}"/>
  </xs:restriction>
</xs:simpleType>
```

73. Le format de ce type de date est aligné sur le code de format 102 selon la norme EDIFACT-ONU, à savoir : AAAAMMJJ.

Où :

- AAAA : l'année à quatre chiffres (par exemple, 1979, 2020) ;
- MM : le mois à deux chiffres, de 01 à 12 en commençant par 01 pour janvier ;
- JJ : le jour du mois à deux chiffres, de 01 à 31.

Exemples :

- Le 1er janvier 1970 est codé « 19700101 » ;
- Le 29 février 2020 est codé « 20200229 » ;
- Le 31 décembre 2045 est codé « 20451231 ».

74. Le champ de la date contient également un attribut facultatif nommé formatCode dont la valeur est donc toujours « 102 ». Ce format ne tient pas compte des fuseaux horaires, et la date doit être considérée comme valable dans tous les fuseaux horaires.

Le code XML ci-dessous présente un exemple de champ comportant uniquement une date.

Expiration d'une garantie le 1er août 2024

```
<ExpirationDateTime formatCode="102">20240801</ExpirationDateTime>
```

2. Champs comprenant une date et une heure

75. Dans les fichiers XSD (XML Schema Definition), ce type de champ est nommé EtirDateTimeType et est défini comme suit, avec les types dont il hérite :

Définition du type EtirDateTimeType

```
<xs:complexType name="EtirDateTimeType">
  <xs:simpleContent>
    <xs:extension base="ds:DateTimeType_208_S">
      <xs:attribute name="formatCode" use="optional">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="208"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:simpleType name="DateTimeType_208_S">
  <xs:restriction base="ds:DateTimeType_S">
    <xs:pattern value="[1-9][0-9][0-9][0-9](([0][1|3|5|7|8])([0][1-9]|[1-2][0-9]|[3][0-1])|([0][4|6|9])([0][1-9]|[1-
2][0-9]|[3][0])|([0][2])([0][1-9]|[1-2][0-9])|([1][0|2])([0][1-9]|[1-2][0-9]|[3][0-1])|([1][1])([0][1-9]|[1-2][0-
9]|[3][0]))(([0-1][0-9])|(2[0-3]))[0-5][0-9](([0-5][0-9]|60))[\-+]((0[0-9])|(1[0-4]))[0-5][0-9]"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="DateTimeType_S">
  <xs:restriction base="xs:string">
    <xs:pattern value=".{1,35}"/>
  </xs:restriction>
</xs:simpleType>
```

76. Le format de ce type de date est conforme au code de format 208 selon la norme EDIFACT-ONU, à savoir : CCYYMMDDHHMMSSZHHMM.

Où, dans l'ordre :

- CCYY : l'année à quatre chiffres (par exemple, 1979, 2020) ;
- MM : le mois à deux chiffres, de 01 à 12 en commençant par 01 pour janvier ;
- DD : le jour du mois à deux chiffres, de 01 à 31 ;
- HH : l'heure du jour à deux chiffres, de 00 (pour minuit) à 23 (pour 23 h) ;
- MM : les minutes de l'heure à deux chiffres, de 00 à 59 ;
- SS : les secondes de la minute à deux chiffres, de 00 à 59 (60 est également autorisé dans le cas d'une seconde intercalaire) ;
- Z : l'introduction du fuseau horaire par un « + » ou un « - » (si le fuseau horaire n'a pas de décalage, un « + » ou un « - » peut être utilisé) ;
- HH : les heures de décalage du fuseau horaire, de 01 à 14 ;
- MM : les minutes de décalage du fuseau horaire, de 00 à 59.

Exemples :

- Le 1er janvier 1970 à 0 h 0 m 0 s à Londres (décalage horaire : +0 h) est codé « 19700101000000+0000 » ;
- Le 29 février 2020 à 9 h 45 m 36 s à New York (décalage horaire : -5 h) est codé « 20200229094536-0500 » ;
- Le 31 décembre 2045 à 22 h 6 m 59 s à Tarawa-Sud, Kiribati (décalage horaire : +14 h) est codé « 20451231220659+1400 ».

77. Le champ comportant la date et l'heure contient également un attribut facultatif nommé **formatCode** dont la valeur est donc toujours « 208 ».

Le code XML ci-dessous présente un exemple de champ comportant la date et l'heure.

Expiration d'une garantie le 1er juillet 2021 à 10 h 3 m 42 s à Istanbul (décalage horaire : +3 h)

```
<ExpirationDateTime formatCode="102">20210701100342+0300</ExpirationDateTime>
```

F. Gestion des erreurs

1. Introduction à la gestion des erreurs

78. Lorsque le système international eTIR reçoit et traite un message, il effectue une série de validations sur le message lui-même, en lien avec la garantie, le titulaire ou le transport associés au message, et il envoie une réponse au système qui a initialement envoyé le message. En cas d'échec pendant ces étapes de validation et de traitement, une liste d'erreurs est renvoyée dans la réponse. Chacune de ces erreurs est présentée sous la forme d'un code d'erreur accompagné d'un pointeur pouvant servir à renvoyer vers un élément XML particulier du message. La liste de tous les codes d'erreur est disponible sur le site rassemblant la documentation du système eTIR.

2. Présentation des codes d'erreur

79. La liste des codes d'erreur est propre au système eTIR, ce qui permet aux équipes informatiques de mieux comprendre les erreurs pendant la mise en place de l'interconnexion au système international eTIR. Cela devrait permettre une mise en œuvre plus rapide, dans l'ensemble, et un traitement plus précis des erreurs provenant du système qui envoie des messages au système international eTIR. De plus, un système de codes d'erreur détaillés simplifiera considérablement la communication entre les parties prenantes et les services d'assistance eTIR, en cas d'incident, afin de repérer et de corriger le problème sous-jacent. La liste des codes d'erreur se fonde sur les meilleures pratiques du secteur de l'informatique. Comme dans la liste des codes d'état HTTP, tous les codes d'erreur comportent trois chiffres, et le premier chiffre du code d'état définit le type d'erreur :

- **1XX − Validation :** validation du message et de ses paramètres ;
- **2XX − Exécution :** problème liés à l'exécution du processus ;
- **3XX − Fonctionnel :** autres problèmes fonctionnels ;
- **4XX − Interne :** problèmes internes au système international eTIR.

80. Chaque type d'erreur est associé à un code d'erreur par défaut qui indique au moins le type d'erreur si le système ne peut pas envoyer de code d'erreur plus explicite.

3. Exemples d'erreurs

81. Voici un exemple de réponse signalant une seule erreur :

Élément obligatoire manquant

```
<ns14:Error>
   <ns14:ValidationCode>101</ns14:ValidationCode>
   <ns14:Pointer>
      <ns14:SequenceNumeric>1</ns14:SequenceNumeric>
      <ns14:Location>/InterGov/ObligationGuarantee/ReferenceID</ns14:Location>
   </ns14:Pointer>
</ns14:Error>
```

82. Ici, l'élément ValidationCode correspond au code d'erreur et l'attribut DocumentSectionCode à l'intérieur de l'élément Pointer renvoie à l'élément problématique de la demande selon la syntaxe XPath.

83. Lorsque plusieurs erreurs du même type sont signalées, le système international eTIR signale une seule erreur, avec une liste de pointeurs.

Exemple avec plusieurs éléments obligatoires manquants

```
<ns14:Error>
   <ns14:ValidationCode>101</ns14:ValidationCode>
   <ns14:Pointer>
      <ns14:SequenceNumeric>1</ns14:SequenceNumeric>
      <ns14:Location>/InterGov/ObligationGuarantee/ReferenceID</ns14:Location>
   </ns14:Pointer>
   <ns14:Pointer>
      <ns14:SequenceNumeric>2</ns14:SequenceNumeric>
      <ns14:Location>/InterGov/ObligationGuarantee/Surety/ID</ns14:Location>
   </ns14:Pointer>
</ns14:Error>
```

84. Enfin, à titre d'exemple, voici une réponse complète à un message I1 (Accepter la garantie) contenant plusieurs erreurs :

Exemple du corps complet d'un message I2 (Résultats de l'acceptation de la garantie) dans lequel plusieurs erreurs sont signalées

```
<soap:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
          wsu:Id="id-30706360-7e18-4764-b080-05364eb55892">
    <ns3:acceptanceResults xmlns:ns4="etir:I2:v4.3" xmlns:ns5="etir:MetaData_DS:v4.3" >
        <ns4:InterGov>
            <ns4:FunctionCode>27</ns4:FunctionCode>
            <ns4:FunctionalReferenceID>bc26c1b8-7392-4d44-9899-317fd72206eb</ns4:FunctionCode>
            <ns4:TypeCode>I2</ns4:TypeCode>
            <ns4:Error>
               <ns5:ValidationCode>102</ns5:ValidationCode>
               <ns5:Pointer>
                  <ns5:SequenceNumeric>1</ns5:SequenceNumeric>
                  <ns5:Location>/InterGov/FunctionCode</ns5:Location>
               </ns5:Pointer>
               <ns5:Pointer>
                  <ns5:SequenceNumeric>2</ns5:SequenceNumeric>
                  <ns5:Location>/InterGov/TypeCode</ns5:Location>
               </ns5:Pointer>
            </ns4:Error>
            <ns4:Error>
               <ns5:ValidationCode>101</ns5:ValidationCode>
               <ns5:Pointer>
                  <ns5:SequenceNumeric>3</ns5:SequenceNumeric>
                  <ns5:Location>/InterGov/ObligationGuarantee/ReferenceID</ns5:Location>
               </ns5:Pointer>
               <ns5:Pointer>
                  <ns5:SequenceNumeric>4</ns5:SequenceNumeric>
                  <ns5:Location>/InterGov/ObligationGuarantee/Surety/ID</ns5:Location>
               </ns5:Pointer>
            </ns4:Error>
        </ns4:InterGov>
    </ns3:acceptanceResults>
</soap:Body>
```

4. Traitement des erreurs

85. Chaque système douanier national connecté au système international eTIR doit traiter correctement les erreurs signalées dans le message de réponse. Lors de la mise en œuvre des différentes paires de messages eTIR, il pourra être pratique, pour les développeurs, de se reporter à la page des codes d'erreur eTIR, en particulier à la colonne « Observations » dans les tableaux, pour savoir quels codes d'erreur pourraient être signalés. À réception des messages du système international eTIR, les erreurs doivent être traitées de telle sorte que les informations pertinentes soient transmises aux systèmes douaniers nationaux concernés. Étant donné que toutes les erreurs sont critiques et empêchent le traitement du message, les utilisateurs des systèmes douaniers nationaux devront prendre les mesures adéquates pour y donner suite.

86. Il en va de même pour les systèmes douaniers nationaux, qui peuvent signaler des erreurs au système international eTIR s'ils reçoivent des demandes qu'ils ne peuvent pas traiter (cela peut être le cas pour les paires de messages suivantes : I15/I16, E9/E10, E11/E12 et E13/E14). Les systèmes douaniers nationaux doivent suivre les spécifications décrites ci-dessus pour signaler des erreurs au système international eTIR lors de l'envoi des messages de réponse.